(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 December 2003 (24.12.2003)

PCT

(10) International Publication Number
WO 03/107242 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US03/18531

(22) International Filing Date: 12 June 2003 (12.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/388,094 12 June 2002 (12.06.2002) US

(71) Applicant: **CARDINALCOMMERCE CORPORATION** [US/US]; 6119 Heisley Road, Mentor, OH 44060-1837 (US).

(72) Inventors: **KERESMAN, Michael, A.**; 8890 Cardinal Drive, Kirtland Hills, OH 44060-1837 (US). **SHERWIN, Francis, M.**; 3377 East Monmouth Road, Cleveland Heights, OH 44118 (US). **BALASUBRAMANIAN, Chandra, S.**; 5779 South Winds Drive, Apt. 77, Mentor-on-the-lake, OH 44060 (US).

(74) Agent: **CORNELY, John, P.**; Fay, Sharpe, Fagan, Minnich & McKee, LLP, 1100 Superior Avenue, Seventh floor, Cleveland, OH 44114-2579 (US).

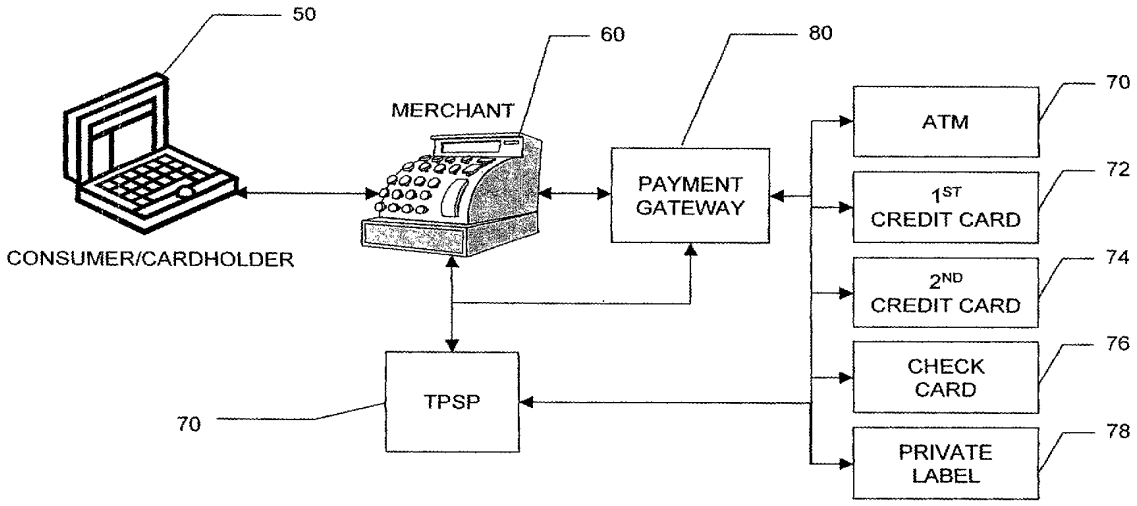
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: UNIVERSAL MERCHANT PLATFORM FOR PAYMENT AUTHENTICATION



(57) Abstract: A consumer shops at an online merchant (60) using a selected payment instrument. Transaction details are sent from the merchant (60) to a transaction processing service provider, TSP (70) that formats and routes various tasks and messages in accordance with authentication protocols prescribed by the payment processing network to which the payment instrument being used for the translation belongs. Payment processing networks include for ATM card (70), first credit card (72), second credit card (74), check card (76) and private label credit card (78). The TPSP (70) obtains transactions from the merchant and distributes them to the proper payment processing networks. Having obtain an authentication determination, the authentication service provider (70) then returns authentication data to the merchant (60) to the established underlying payment processing infrastructure via optional payment gateway (80).

WO 03/107242 A1

UNIVERSAL MERCHANT PLATFORM FOR PAYMENT AUTHENTICATION

[0001] This application claims the benefit of U.S. Provisional Application No. 60/386,345, filed June, 12 2002, incorporated herein by reference in its entirety.

Field

[0002] The present invention relates to the art of authentication. It finds particular application in conjunction with facilitating the authentication of an individual to conduct a secure commercial transaction with credit or debit card over a communications network, e.g., the Internet, and will be described with particular reference thereto. It is to be appreciated, however, that the invention is also amenable to other like applications.

Background

[0003] Internet commerce, or e-commerce as it is otherwise known, relates to the buying and selling of products and services between consumers and merchants over the Internet or other like transactional exchanges of information. The convenience of shopping over the Internet has sparked considerable interest in e-commerce on behalf of both consumers and merchants. Internet sales, or like transactions, have been typically carried out using standard credit cards such as Visa®, MasterCard®, Discover®, American Express®, or the like, or standard debit cards, i.e., check cards or automated teller machine (ATM) cards which directly access funds from an associated deposit account or other bank account.

[0004] While widely used for more traditional face-to-face transactions, use of these standard cards in connection with e-commerce presents certain difficulties, including difficulties concerning authentication or positive identification of the cardholder. For example, maintaining consumer confidence in security has become difficult with increased reports of fraud. The resulting apprehension is also fueled by consumer uncertainty of the reputation or integrity of a merchant with whom the consumer is dealing. Questionable security of the consumer's card information or

other personal information typically submitted along with a traditional e-commerce transaction (e.g., address, card number, phone number, etc.) serves to increase apprehension even more. Additionally, cardholders, merchants and financial institutions are all concerned about safeguarding against fraudulent or otherwise unauthorized transactions.

[0005] Accordingly, various credit card networks have implemented initiatives or programs aimed at safeguarding against fraud. For example, Visa® and MasterCard® both support authentication initiatives whereby a cardholder is authenticated by the bank or financial institution issuing the card, i.e., the issuing bank. FIGURE **1**, illustrates one such exemplary authentication initiative. As shown in this example, a consumer/cardholder **10**, e.g., employing a suitable web browser or the like, is making an on-line purchase, e.g., over the Internet, from a merchant **20**. As is known in the art, the illustrated back-end payment processing chain includes an optional payment gateway **30**, the merchant's financial institution or acquiring bank **32**, the credit card network **34** and the issuing bank **36**.

[0006] At a point of checkout, the consumer **10** selects an appropriate payment method based on the initiatives supported by the merchant **20**. At this point, the consumer fills out the on-line checkout form including a payment option, card number, expiration date, etc. Based on the payment information, the merchant **20**, via a plug-in **22** installed on their server, passes a verify enrollment request (VEReq) message to a directory **38** on a server, e.g., suitably operated by the credit card network **34**. The directory **38** includes a database associating participating merchants with their acquiring banks and a database associating card number ranges with locations or addresses, e.g., universal resource locator (URL) addresses, of issuing banks' authentication servers, e.g., the authentication server **40** for issuing bank **36**. The VEReq message is a request to verify the enrollment of the card in the authentication program, and it contains the card number provided by the consumer **10**.

[0007] Based on the card number range stored within the directory, the VEReq message will be sent to the appropriate URL address for the server **40** which returns to the merchant **20** via the directory **38** a response thereto, i.e., a verify enrollment response (VERes). That is to say, the server **40** will verify the enrollment

status of the card and respond with a VERes message to the directory **38** which is then passed back to the merchant's plug-in component **22**.

[0008] Based on the VERes message (i.e., if positive), the merchant plug-in component **22** will redirect the cardholder's browser to the server **40** by passing it a payer authentication request (PAReq) message generated by the merchant's plug-in component **22**. The consumer **10** then completes an authentication process directly with the server **40**. The authentication server **40** authenticates the consumer/cardholder **10** and responds to the merchant **20** with a payer authentication response (PARes) message including a digital signature. The merchant's plug-in component **22** validates the digital signature of the PARes and extracts the authentication status and other specified data that is to be used by the merchant **20** during the payment authorization process carried out via the back-end payment processing chain. For example, the merchant **20** sends an authorization/sale transaction to their payment gateway **30** along with the data elements received from the PARes. The payment gateway **30** routes the data to the acquiring bank **32** based on the acquirer's specification. The acquiring bank **32** then sends the data via the appropriate credit card network **34** to the issuing bank **36** for settlement.

[0009] When using authentication initiatives such as the aforementioned example, the credit card network often ensures participating merchants that fraudulent transactions and other charge backs, as they are known in the art, will not be the merchants' responsibility provided the specified protocols have been followed. However, there are considerable burdens placed upon the merchants to participate in the authentication initiatives. For example, typical installation of the merchant plug-in can be overly burdensome using up resources, i.e., computing power, memory, data storage capacity, etc., the merchant would otherwise prefer to devote to other tasks. Often, the plug-in component can be extremely large and/or cumbersome to implement on the merchant's server. Moreover, for a merchant that participates in a plurality of such authentication programs for multiple credit card networks, the burden can be that much more, i.e., requiring a separate plug-in component for each individual authentication initiative they wish to support, especially considering that each credit card network may have its own particular

protocols, data fields that are employed in the respective messages, specific data format requirements, etc.

[0010] Further, the merchants are responsible for remaining current with initiative protocols that can change periodically. That is to say, as the authentication protocols are updated and/or changed by the respective credit card networks, the merchants are likewise responsible for updating and/or changing their plug-in components to reflect those update and/or changes being mandated by the credit card networks.

[0011] The present invention contemplates a new and improved system and/or method which overcomes the above-referenced problems and others.

Summary

[0012] In accordance with one aspect of the present invention, a method is provided for processing authentication of a consumer using one of a plurality of different types of payment instruments to conduct a commercial transaction over a communications network with a merchant. The payment instrument being used is either enrolled in or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment instruments by payment networks supporting the same. The method includes: obtaining payment information for the transaction from the merchant, the payment information including a number identifying the particular payment instrument being used; determining the type of payment instrument being used from the payment information; obtaining an authentication determination for the transaction in accordance with the authentication protocols prescribed for the determined type of payment instrument being used; and, returning the obtained authentication determination to the merchant.

[0013] In accordance with another aspect of the present invention, a system is provided for supporting authentication processing of commercial transactions conducted over a communications network between a consumers and merchants. The consumers are each using one of a plurality of different types of payment instruments, the used payment instrument being either enrolled or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment

instruments. The system includes: a connection layer for connecting with the merchants to exchange communications therewith, the connection layer receiving payment information for the transactions from the merchants, the payment information for each transaction including a number identifying the particular payment instrument being used; a plug-in layer including a plurality of plug-in components, each plug-in component administering a different one of the authentication programs in accordance with the authentication protocols prescribed to obtain an authentication determination for the transactions; and, a distribution layer residing between the connection layer and the plug-in layer, the distribution layer routing communications between the connection layer and selected plug-in components in the plug-in layer, wherein the payment information for each transaction is routed to the plug-in component responsible for administering the authentication program for the particular payment instrument used for that transaction.

[0014] In accordance with yet another aspect of the present invention, a system is provided for processing authentication of a consumer using one of a plurality of different types of payment instruments to conduct a commercial transaction over a communications network with a merchant. The payment instrument being used is either enrolled in or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment instruments by payment networks supporting the same. The system includes: means for obtaining payment information for the transaction from the merchant, the payment information including a number identifying the particular payment instrument being used; means for determining the type of payment instrument being used from the payment information; means for obtaining an authentication determination for the transaction in accordance with the authentication protocols prescribed for the determined type of payment instrument being used; and, means for returning the obtained authentication determination to the merchant.

[0015] Numerous advantages and benefits of the present invention will become apparent to those of ordinary skill in the art upon reading and understanding the present specification.

Brief Description of the Drawings

[0016] The present invention may take form in various components and arrangements of components, and/or in various steps and arrangements of steps. The drawings are only for purposes of illustrating preferred embodiments and are not to be construed as limiting the invention.

[0017] FIGURE **1** is a block diagram illustrating a typical e-commerce transaction carried out in accordance with an exemplary authentication initiative/program of a credit card network.

[0018] FIGURE **2** is a diagrammatic illustration showing a high level overview of an exemplary processing of an authenticated commercial transaction in accordance with aspects of the present invention.

[0019] FIGURE **3** is a block diagram illustrating an exemplary merchant server and exemplary merchant authentication processing system in accordance with aspects of the present invention.

Detailed Description of Preferred Embodiments

[0020] For clarity and simplicity, the present specification shall refer to structural and/or functional network elements, entities and/or facilities, relevant standards, protocols and/or services, and other components that are commonly known in the art without further detailed explanation as to their configuration or operation except to the extent the same has been modified or altered in accordance with and/or to accommodate aspects of the present invention.

[0021] In accordance with a preferred embodiment, the present invention serves as a centralized merchant processing system for authenticated payments, allowing a merchant to securely and easily accommodate authentication of consumers and/or cardholders in accordance with a variety of authentication initiatives implemented by credit card networks, and to process electronic transactions through any payment network using a single platform. It also enables merchants to process these payments, regardless of which payment network they are to be routed through, with a single implementation. In one version, this is accomplished using "thin-client" communication software which links information with a centralized merchant authentication processing system (MAPS) upon demand. Moreover, it allows them or a funding source to use the established underlying

payment processing infrastructure to process their credit/debit instruments at participating merchant sites.

[0022] The advantages to funding sources are: the ability to authenticate users and process all electronic transactions through a single platform; the ability to seamlessly process payments using any given payment network; a reduction in processing costs; increased use of their credit/debit instrument; increased acceptance of their credit/debit instrument; the ability to send authenticated payment and authorization requests to any network; the ability to receive detailed consumer purchasing behavior statistics. Likewise, there are advantages to the merchant, including, but not limited to: the ability to comply with, participate in, and enjoy the benefits of a variety of authentication initiatives; the ability to authenticate consumers using different payment vehicles or credit cards, thereby avoiding lost sales; and, protection from fraud.

[0023] The approach detailed in the present specification provides a secure, scalable and modular solution for merchants to participate in and support various payment authentication initiatives, such as, e.g., Visa's 3-D Secure Verified by Visa (VbV) and MasterCard's SecureCode and/or Secure Payment Application (SPA). It provides payment gateways, acquirers, merchant service providers (MSP) and independent sales organizations (ISO) an easy and effective way to provide their merchants with the means for cardholder authentication, as defined by various authenticating programs, e.g., VbV, SecureCode, SPA, etc.

[0024] With reference to FIGURE **2**, a high level overview of an exemplary commercial transaction carried out in accordance with aspect of the present invention is diagrammatically illustrated. Via a computer, a consumer **50** shops at an on-line merchant **60** using a selected payment instrument. When the transaction is completed, transaction details are sent from the merchant **60** to a transaction processing service provider (TPSP) **70** that formats and routes various messages and takes other defined actions on behalf of the merchant **60** in accordance with authentication protocols prescribed by the payment processing network to which the payment instrument being used for the transaction belongs. For example, as shown, there is an ATM card payment processing network **70**, a first credit card payment processing network **72** for a first type or brand of credit card, a second credit card payment processing network **74** for a second type or brand of credit

card, a check card payment processing network **76**, and a private label credit card processing network **78**, all of which optionally support different authentication protocols. As shown, the TPSP **70** optionally obtains transactions from the merchant and distributes them to the proper payment processing networks, e.g., for direct authentication by the entity issuing the payment instrument used in the transaction. Having obtain an authentication determination, the authentication service provider **70** then returns this determination to the merchant **60** so that it may be included when the transaction is submitted by the merchant **60** to the established underlying payment processing infrastructure, e.g., via an optional payment gateway **80**.

[0025] More specifically, with reference to FIGURE **3**, an exemplary server **100** operated by an on-line merchant and an exemplary merchant authentication processing system (MAPS) **200** are shown. The merchant server **100** includes a checkout processing function **102**, a payment processing function **104** and a thin-client **106** operative to provide interworking between the server **100** and the MAPS **200**. The server **100** suitably hosts a web site accessible over a communications network (e.g., the Internet) by consumers/cardholders to conduct commercial transactions, i.e., to purchase good and/or services. That is to say, a consumer/cardholder using an appropriate web browser or like application may connect to the server **100** over the Internet to shop on the hosted web site.

[0026] Suitably, when a consumer/cardholder is done shopping, the checkout processing function **102** is invoked thereby providing the consumer's web browser with a checkout web page whereby the transaction amount (i.e., the total amount of payment due) is established and/or presented and payment information collected. The checkout processing function **102** supports payment with a plurality of different types of payment instruments, e.g., credit and/or debit cards, belonging to different payment processing networks, e.g., Visa®, MasterCard®, etc. That is to say, the consumer/cardholder optionally selects the particular type of payment instrument being used for the commercial transaction from a plurality of supported payment instrument types. Additionally, the checkout processing function **102** is also used to collect the card number, expiration date, and other relevant data from the consumer/cardholder.

[0027] The payment processing function **104** submits completed transactions to the established underlying payment processing infrastructure (i.e., payment gateway, acquiring bank, payment processing network, issuing bank, etc.) in the usual manner as prescribed by the various payment processing networks.

[0028] The merchant's thin-client **106** is used for communicating transaction data elements such as card number, transaction amount, etc. between the merchant's website and the MAPS **200**. The thin-client is not aware of the specific processing logic or protocols prescribed for each payment authentication initiative. Suitably, the thin-client **106** is a small software component installed on the merchant's server **100**, e.g., approximately 50 kilobytes in size. Alternately, the following options for connecting to the MAPS **200** are also available in order to cater to different merchants depending upon the merchant's transaction processing volume, technical expertise, resource availability and software standards: (i) an "easy connection" implementation, as it is termed herein, i.e., a software-less merchant client; and (ii) a "direct connection" implementation, as it is termed herein, i.e., a direct integration within the MAPS **200**. Nevertheless, the thin-client approach provides the merchant with thin (i.e., small) software object (e.g., approximately 50 kilobytes) that is used by the merchant to communicate with the MAPS **200**. Using the thin-client **106**, the merchant can participate within the various payment authentication initiatives, e.g., VbV, SPA, etc., without any significant reprogramming of the server **100** or their web site. Suitably, the thin-client **106** is available as a COM object or a Java component that is integrated with the merchant's established transaction handling process.

[0029] The thin client software is used by the merchants to securely communicate with the MAPS. The thin client software is used to format name/value pairs to the required MAPS message format and securely communicate the message to the MAPS system. The thin client does not hold any payment authentication specific business process logic. The thin client supports the following features: secure communication to the MAPS **200**, formatting data to the MAPS specific message format, and allowing merchants to access response data.

[0030] Suitably, the architecture of the thin-client **106** includes a request layer **110** and a response layer **112** that sit on top of a message formatting layer **114** that sits on top of a communication layer **116**. The request layer **110** provides an

interface that can be accessed by the merchant's web site to provide data to the thin-client **106** in the form of name/value pairs. The request layer **110** also exposes functions for the merchant to send messages to a specific MAPS **200**. The response layer **112** provides an interface for returning responses to the web site, e.g., returned as a function call response to a send message instruction. The message formatting layer **114** formats and translates traffic between the request and response layers **110** and **112** which employ a name/value pairs format and the communication layer **116** which suitably employs an XML format to communicate with the MAPS **200**. The communication layer **116** provides connectivity with the MAPS **200**, e.g., via HTTPS (i.e., hypertext transfer protocol over secure socket layer (SSL)).

[0031] The MAPS **200** is a core component within the system. The MAPS **200** provides the functionality to merchants for participation in the various different authentication programs and initiatives supported by the payment processing networks. Suitable, the MAPS **200** architecture is extensible to support existing and new releases of existing payment initiatives without requiring a total software rewrite, and likewise accommodates addition of new authentication initiatives. This approach leads to an easy implementation at the merchant website level, i.e., where the processing logic and message handling prescribed by the initiatives are controlled at a central location rather than at an individual merchant level. That is to say, any changes or additions implemented do not affect individual merchants.

[0032] The MAPS **200** provides a secure infrastructure for processing transactions based on payment authentication initiative specifications. The MAPS **200** provides extensible software than can seamlessly support future revisions of the existing payment authentication initiatives and new payment authentication initiatives. Preferably, the MAPS **200** provides complete abstraction as to how each payment authentication initiative is implemented, thereby providing one central location for any changes. Suitably, the MAPS **200** is programmed with Java software to provide the described functionality. The MAPS software architecture includes the following layers: a connectivity layer **210** that sit on top of a message distribution layer **220** that sit on top of a plug-in layer **230**, and external connection layer **240**. The external connection layer **240** provides a generic interface that is

used by the MAPS **200** to communicate with outside resources, e.g., the directory or the like as prescribed by various authentication protocols.

[0033] The connectivity layer **210** provides a generic layer for external entities such as merchants to connect to and process a specific payment authentication transaction. The connectivity layer **210** supports the following connectors: an HTTPS server **212**; a "direct connector" **214**, as it is termed herein; and, an "easy connector" **216**, as it is termed herein; and an optional "other connector" **218**, as it is termed herein.

[0034] The HTTPS server **212** receives and/or sends HTTP messages and communicate them to and/or from the message distribution layer **220**. This connecter is used by the thin-client **106** to communicate with the MAPS **200**. The direct connector **214** provides a Java interface than can be used by a merchant integrating with the MAPS **200** using the direct connection approach. This connector exposes the appropriate Java interfaces than can be used by the merchant during integration. Messages received/sent using this connector are also communicated to/from the message distribution layer **220**. The easy connector **216** provides a web server that is used to communicate with the message distributor and also to communicate with the cardholder. This connector interfaces with the cardholder to perform the merchant functionality and interfaces with the message distributor to communicate the relevant messages. Suitably, the other connector **218** allows the connectivity layer **210** to be expanded to support other communication and custom integration options.

[0035] Implementing multiple connector types provides multiple ways for merchants to integrate and participate within the various authentication initiatives. By providing multiple integration approaches, the a wide variety of merchants can be supported depending upon the merchant's technical expertise, resource availability and transaction processing volume. That is to say, in addition to the thin-client approach, a "direct connection" and "easy connection" approach are also optional available to merchants.

[0036] The direct connection approach is provided for merchants which insist on or otherwise want to host and manage the product, e.g., such merchants may be high transaction volume merchants and/or merchants who have the technical resources to host and manage the product. The merchant can use direct java calls

to interface with the MAPS **200** and communicate the appropriate XML messages. The direct connect interface is also available via a local socket server provided as part of the MAPS **200**. Merchants utilizing a software platform other than Java can use the local socket server. Under the direct connection approach the merchants provide their own hardware and/or software. On the opposite end of the spectrum, the easy connection approach is provided as a software-less integration approach for merchants that do not wish to install the thin-client **106**. Using the easy connect approach, the merchant redirects the cardholder to the MAPS easy connect web server. The web server acts on behalf of the merchant's website and communicates with the MAPS **200** to provide the appropriate processing for the appropriate authentication initiative. Under this approach, the merchant redirects the cardholder using HTTPS posts and receives the responses at a specified response URL. HTTP redirections are be performed via the cardholder's browser. Using the easy connection approach the merchant may place an appropriate script after the cardholder/consumer has provided the merchant with appropriate payment data, such as credit card number, expiration date, etc. The merchant receives the authentication response to the URL specified within an response URL field designated in the script.

[0037] The message distribution layer **220** is a component within the software architecture that facilitates scalability, redundancy, high availability and transaction processing speed. Suitably, the message distribution layer **220** is developed using Java 2 Enterprise Edition (J2EE) specifications related to transaction processing. It is preferably a low footprint message distribution application configured to route XML messages to specific plug-in components in the plug-in layer **230** for appropriate transaction processing.

[0038] The plug-in layer **230** includes a plurality of individual authentication initiative plug-in components **232** that listen to the message distribution layer **220** for a specific message type. The respective plug-in component **232** is activated by the message distribution layer **220** that sends messages to the specified plug-in component **232** based upon the type of payment instrument being used for the transaction being processed. For example, as shown, the MAPS **200** optionally includes plug-in components **232** for Visa®, MasterCard® and other payment instruments. Notably, the plug-in components **232** are freely and easily updated,

exchanged or otherwise manipulated as desired to comply with new version of existing authentication initiatives, or additional plug-in components are freely and easily added to accommodate new initiatives, without any additional alterations to the MAPS **200** or on the merchant side. In this manner, the merchants are automatically kept in compliance with the latest authentication initiatives without having to rework authentication processing protocols on their server **100**. Further, as other payment processing enhancements are introduced and/or desired, e.g., currency conversion, compliant plug-in components therefor may likewise be developed and simply added to the plug-in layer **230** of the MAPS **200** thereby providing the merchant with the particular payment processing functionality.

[0039] Additionally, the plug-in layer **230** optionally also supports various management and/or administrative applications (not shown). For example, a merchant registration application module may be made available to merchant service providers (MSPs) for registering their merchants within the appropriate payment authentication initiatives. Suitably, the merchant registration application offers a web-based application, where the merchants, based on communications received from their MSPs, can register themselves and download appropriate software and related integration documentation. The merchant registration application also provides registration/license key-based control to the MSP, where the MSP can communicate a license key to the merchant that will be used to authenticate the merchant during registration and download. Optionally, the data elements collected from the merchants can be customized as desired by the MSP.

[0040] An optional MSP administration application provides the MSP with a web-based application that is used to administer merchants. The MSP administration application may, e.g., provides the following features: enabling/disabling merchants for use of the MAPS **200**; maintaining merchant profile information; etc. The MSP administration application is optionally accessed directly via XML/HTTP based application program interfaces (APIs) that may also be used to integrate with other systems. Additionally, a merchant self-service application allows the merchant to access their profile information via the web. For example, the merchant self-service application optionally offers the following features: self profile management; access to transaction history; access to raw message logs related to authentication processes; etc. The merchant self-service

application may be similarly accessed directly via XML/HTTP based APIs that are optionally also used to integrate with other systems.

[0041] As another option, a MSP reporting application provides a web-based application for MSPs to view consolidated and individual transaction listings. For example, the following reports may optionally be provided as part of the MSP reporting application: consolidated transaction count/dollar volume reports; individual transaction reports; raw message logs; merchant registration reports; and/or other customized reports.

[0042] As will be appreciated by those of ordinary skill in the art, the MAPS **200** provides a method for authenticating a consumer using one of a plurality of different types of payment instruments (e.g., credit/debit cards) to conduct a commercial transaction over a communications network with a merchant employing the MAPS **200**. The payment instrument may be either enrolled in or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment instruments by payment networks supporting the same.

[0043] Suitably, via the thin-client approach (or alternately the direct or easy connection approaches) the MAPS **200** obtains payment information for the transaction from the merchant's server **100**. Suitably, the payment information includes a number identifying the particular payment instrument being used (i.e., the card number), an expiration date, transaction details (i.e., the transaction amount, etc), and other pertinent data. In the case of the thin-client approach, the payment information is obtained from the merchant's web site or page via the request layer **110** in the form of name/value pairs. The request layer **110** passes the payment information to the message formatting layer **114** that translates it into an XML formatted message and passes it to the communication layer **116**. The communication layer **116** then passes the message in the XML format to the MAPS **200** via the HTTPS server **212** in the connectivity layer **210**.

[0044] Upon receiving the payment information, the MAPS **200** determines the type of payment instrument being used from the payment information. Notably, the payment processing network to which a credit/debit card belongs can be determined from the card number as is known in the art.

[0045] Optionally, the MAPS **200** determines from the enrollment status of the particular payment instrument being used for the transaction. For example, the MAPS **200** may maintain a local cache or database of card numbers that identifies those payment instruments enrolled in for participation in various authentication programs and/or initiatives. If the particular payment instrument being used is not enrolled in a particular authentication program for the determined type of payment instrument, then the process may be ended at this point with the MAPS **200** retuning a "not enrolled" message or data back to the thin-client **106** installed on the merchant's server **100**. Accordingly, the thin-client **106** passes this information to the payment processing function **104** to be bundled with the transaction data for submission of the completed transaction to the established underlying payment processing infrastructure. It is to be appreciated, that the returned "not enrolled" message or data, as with all such information returned to the merchant, is provided by the MAPS **200** through the thin-client **106** (i.e., through the communication layer **116**, the message formatting layer **114** and the response layer **112**) such that it emerges already formatted and/or otherwise in compliance with the appropriate authentication protocols prescribed so that the merchant does not have to manipulate the data further prior to submission to the established underlying payment processing infrastructure.

[0046] Alternately, if the particular payment instrument being used is enrolled in an authentication program for the determined type of payment instrument, then the payment information is passed to the message distribution layer **220** that routes it to the proper plug-in component **232** in the plug-in layer **230**. The plug-in component **232** then handles, administers and/or otherwise executes set procedures prescribed for the respective authentication program employing the appropriate protocols and/or logic to obtain an authentication determination for the transaction. For example, the plug-in component **232** formats and routes messages in accordance with the authentication protocols prescribed for the determined type of payment instrument being used. Having obtained the authentication determination, the MAPS **200** returns the same to the merchant's server **100**.

[0047] Suitably, the plug-in components **232** are programmed to administer any of a variety of authentication protocols as may be prescribed for different types of payment instruments support be various payment processing networks. For

example, to accommodate a particular authentication initiative, a particular plug-in component **232** optionally formats and routes a messages to an issuing entity, e.g., an issuing bank having issued the particular payment instrument being used for the transaction, requesting that the issuing entity confirm the enrollment status of the particular payment instrument being used for the transaction. Upon obtaining a response to the enrollment request message from the issuing entity, the information may be returned to the merchant's server **100** in the same manner as if the MAPS **200** performed the enrollment check itself.

[0048] Additionally, once the enrollment status is determined to be positive, the operative plug-in component **232** optionally formats and routes a second message to the merchant such that the consumer/cardholder is redirected to the issuing entity for completing authentication directly therewith, whereupon the authentication determination is made. A response containing the authentication determination made by the issuing entity is then returned in accordance with routing instructions contained in the second message so that it is obtained by the MAPS **200**. Suitably, the routing instructions include a universal resource locator (URL) directing the response back to the MAPS **200**. Optionally, the plug-in component **232** verifies that the response to the second message was obtained from the issuing entity, e.g., by checking a digital signature incorporated with the response. The MAPS **200** is also optionally equipped to detect and/or qualitatively evaluate the level and/or type of authentication employed to arrive at the authentication determination, and this information may be communicated to the merchant or others.

[0049] To further comply with another selected authentication initiative, a particular plug-in component **232** is optionally programmed such that the MAPS **200** is equipped to dynamically add one or more data fields to the merchant's web page so as to bring the merchant's web page into conformity with prescribed authentication protocols for the determined type of payment instrument. Additionally, other data elements and/or fields may optionally be dynamically added, e.g., to provide currency conversion, etc.

[0050] Suitably, the MAPS **200** further includes a database (not shown) in which historical records of transactions processed by the MAPS **200** are maintained. The historical records can then be optionally accessed by the merchants or MSPs to perform audit trail and/or reconciliation operations.

[0051] It is to be appreciated that the foregoing description and the accompanying FIGURES are merely exemplary in nature. In particular, other hardware and/or software configurations recognizable to one of ordinary skill in the art may be employed to implement the present invention, and other similar payment authentication initiatives, i.e., other than the exemplary VbV and SPA, may likewise be supported without departing from the scope of the present invention. Nevertheless, the architecture described in the present specification achieves certain benefits. For example, the availability of multiple implementation approaches (i.e., thin-client, direction connection and easy connection) allows a customized fit to a variety of differently equipped merchants based upon their transaction processing volume, technical expertise, software and/or hardware resources, etc. Further, the centralized MAPS **200** removes the burden otherwise placed on the merchant's server **100** having to support multiple payment processing initiatives providing substantially complete abstraction related to individual payment authentication initiative processing rules and logic, and with its extensible plug-in layer **230**, provides availability to multiple payment authentication initiatives with one implementation on the merchant side.

[0052] Additionally, where the merchant employs a MSP to perform payment processing and/or related tasks on the merchant's behalf, it is to be appreciated that the MSP may effectively step into the position of the merchant relative to the MAPS **200**. For example, rather than the thin-client **106** being installed on the individual merchant's server **100**, it may be installed on the MSP's server which may use it on behalf of a single merchant or multiple merchants serviced by the MSP. That is to say, information and/or data to and/or from respective merchants would first be routed through the MSP's server where it is exposed to and/or interacts with the thin-client **106** installed thereon in essentially the same manner as described above.

[0053] The invention has been described with reference to the preferred embodiments. Obviously, modifications and alterations will occur to others upon a reading and understanding of this specification. It is intended that the invention be construed as including all such modifications and alterations insofar as they come within the scope of the appended claims or the equivalents thereof.

Claims

[0054] What is claimed is:

1. A method for processing authentication of a consumer using one of a plurality of different types of payment instruments to conduct a commercial transaction over a communications network with a merchant, wherein the payment instrument being used is either enrolled in or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment instruments by payment networks supporting the same, the method comprising:

(a) obtaining payment information for the transaction from the merchant, said payment information including a number identifying the particular payment instrument being used;

(b) determining the type of payment instrument being used from the payment information;

(c) obtaining an authentication determination for the transaction in accordance with the authentication protocols prescribed for the determined type of payment instrument being used; and,

(d) returning the obtained authentication determination to the merchant.

2. The method of claim **1**, further comprising:

formatting messages in accordance with the authentication protocols prescribed for the determined type of payment instrument being used; and,

routing the messages in accordance with the authentication protocols prescribed for the determined type of payment instrument being used.

3. The method of claim **2**, wherein the formatted messages includes a first message that is routed to an issuing entity, said issuing entity having issued the particular payment instrument being used for the transaction and said first message requesting that the issuing entity confirm an enrollment status of the particular payment instrument being used for the transaction.

4. The method of claim **3**, further comprising obtaining a response to the first message from the issuing entity, wherein based upon the response, if the particular payment instrument being used is not enrolled in the authentication program for the determined type of payment instrument, then steps (c) and (d) are omitted, otherwise if the particular payment instrument being used is enrolled in the authentication program for the determined type of payment instrument, then steps (c) and (d) are completed.

5. The method of claim **4**, wherein the formatted messages include a second message that is routed to the merchant such that the consumer is redirected to the issuing entity for completing authentication directly therewith whereupon the authentication determination is made, a response to said second message containing the authentication determination made by the issuing entity being returned in accordance with routing instructions contained in the second message so that it is obtained in step (c).

6. The method of claim **5**, further comprising:

verifying that the response to the second message was obtained from the issuing entity.

7. The method of claim **1**, wherein the consumer accesses a merchant's web page over the communications network to conduct the commercial transaction, and step (c) comprises:

dynamically adding one or more data fields to the merchant's web page.

8. The method of claim **1**, wherein the payment information is obtained in extensible Markup Language (XML) format.

9. The method of claim **1**, further comprising:

determining from the payment information an enrollment status of the particular payment instrument being used for the transaction, wherein if the particular payment instrument being used is not enrolled in the authentication program for the determined type of payment instrument, then steps (c) and (d) are

omitted, otherwise if the particular payment instrument being used is enrolled in the authentication program for the determined type of payment instrument, then steps (c) and (d) are completed.

10. The method of claim **1**, wherein the payment instrument is a credit or debit card.

11. A system for supporting authentication processing of commercial transactions conducted over a communications network between a consumers and merchants, wherein the consumers are each using one of a plurality of different types of payment instruments, said used payment instrument being either enrolled or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment instruments, the system comprising:

a connection layer for connecting with the merchants to exchange communications therewith, said connection layer receiving payment information for the transactions from the merchants, said payment information for each transaction including a number identifying the particular payment instrument being used;

a plug-in layer including a plurality of plug-in components, each plug-in component administering a different one of the authentication programs in accordance with the authentication protocols prescribed to obtain an authentication determination for the transactions; and,

a distribution layer residing between the connection layer and the plug-in layer, said distribution layer routing communications between the connection layer and selected plug-in components in the plug-in layer, wherein said payment information for each transaction is routed to the plug-in component responsible for administering the authentication program for the particular payment instrument used for that transaction.

12. The system of claim **11**, wherein the connection layer supports a plurality of connection means allowing for different types of connectivity with the merchant.

13. The system of claim **12**, wherein at least one of the connection means is an HTTPS server that communicates with a thin-client installed on a server that is supporting a web site of the merchant, said thin-client providing communication with the web site.

14. The system of claim **11**, wherein the plug-in layer is extensible so as to allow selected plug-in components to be added, removed and modified without disrupting other plug-in components residing in the plug-in layer.

15. A system for processing authentication of a consumer using one of a plurality of different types of payment instruments to conduct a commercial transaction over a communications network with a merchant, wherein the payment instrument being used is either enrolled in or not enrolled in an authentication program conforming to one of a plurality of authentication protocols prescribed for the respective plurality of different types of payment instruments by payment networks supporting the same, the system comprising:

means for obtaining payment information for the transaction from the merchant, said payment information including a number identifying the particular payment instrument being used;

means for determining the type of payment instrument being used from the payment information;

means for obtaining an authentication determination for the transaction in accordance with the authentication protocols prescribed for the determined type of payment instrument being used; and,

means for returning the obtained authentication determination to the merchant.

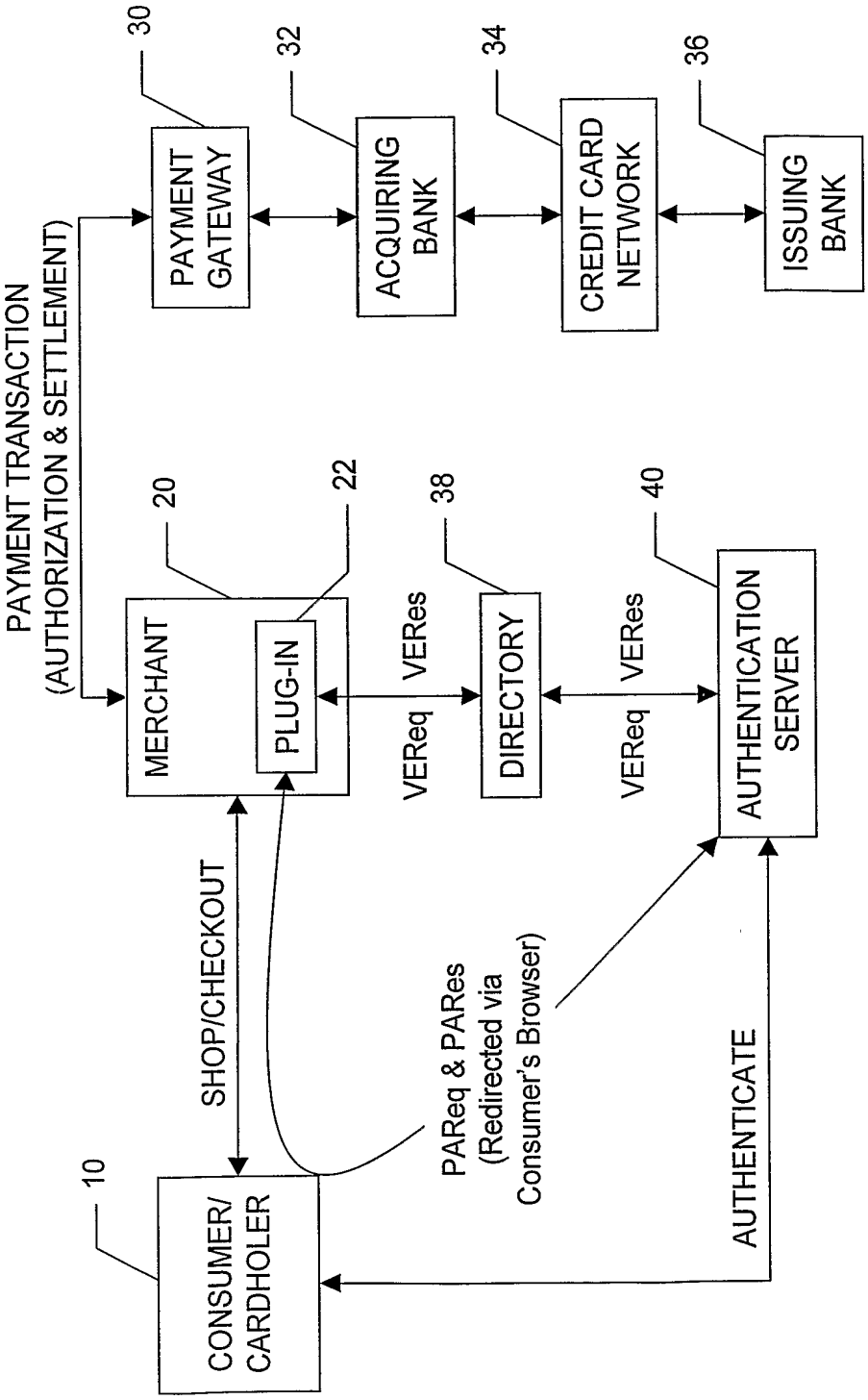

PAYMENT TRANSACTION
(AUTHORIZATION & SETTLEMENT)
30
PAYMENT GATEWAY
32
ACQUIRING BANK
34
CREDIT CARD NETWORK
36
ISSUING BANK
20
MERCHANT
22
PLUG-IN
38
DIRECTORY
40
AUTHENTICATION SERVER
VEReq
VERes
VEReq
VERes
SHOP/CHECKOUT
PAReq & PARes
(Redirected via
Consumer's Browser)
AUTHENTICATE
10
CONSUMER/
CARDHOLER

FIGURE 1

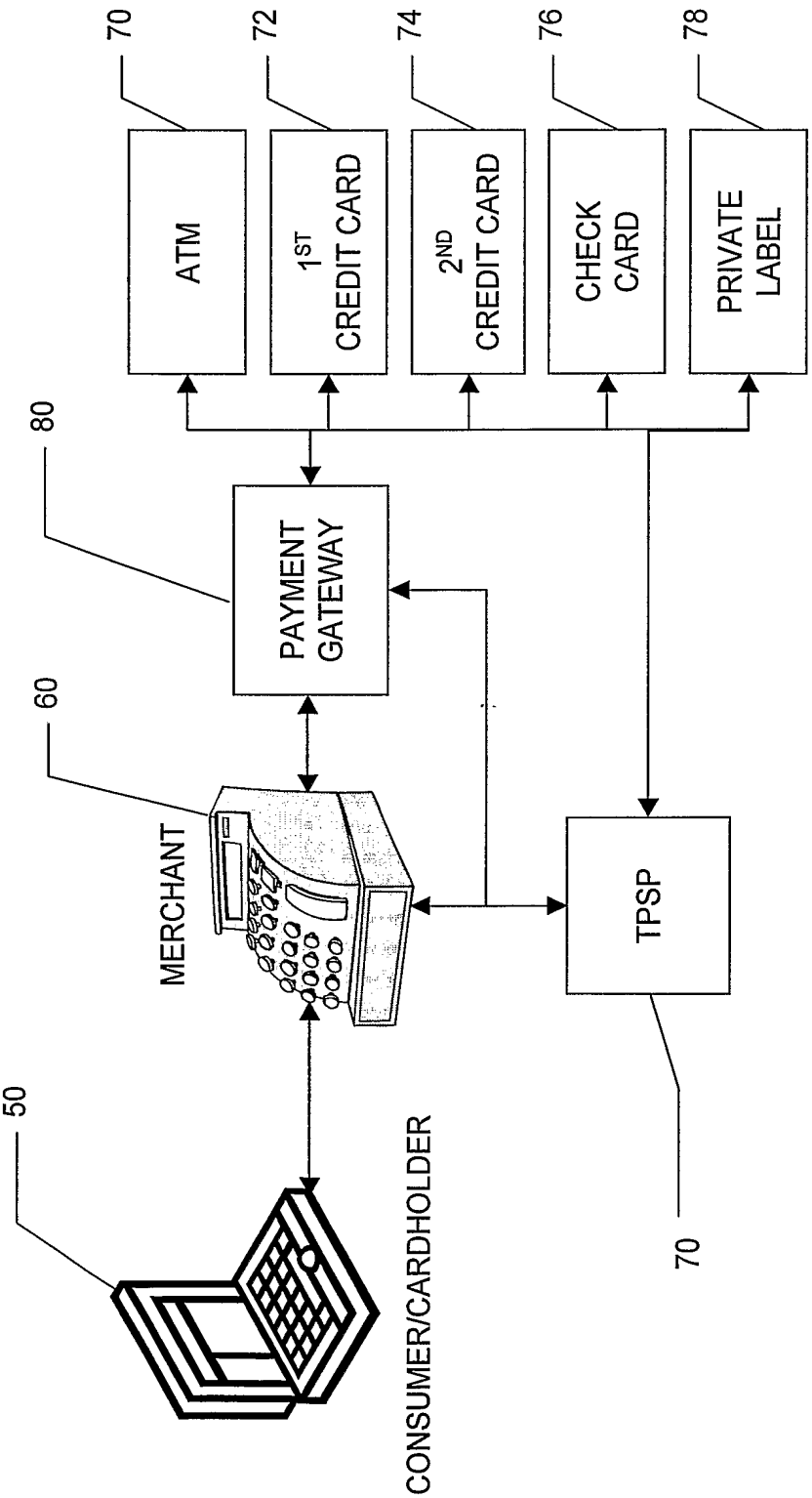

70
72
74
76
78
ATM
1ST CREDIT CARD
2ND CREDIT CARD
CHECK CARD
PRIVATE LABEL
80
PAYMENT GATEWAY
60
MERCHANT
TPSP
50
CONSUMER/CARDHOLDER
70

FIGURE 2

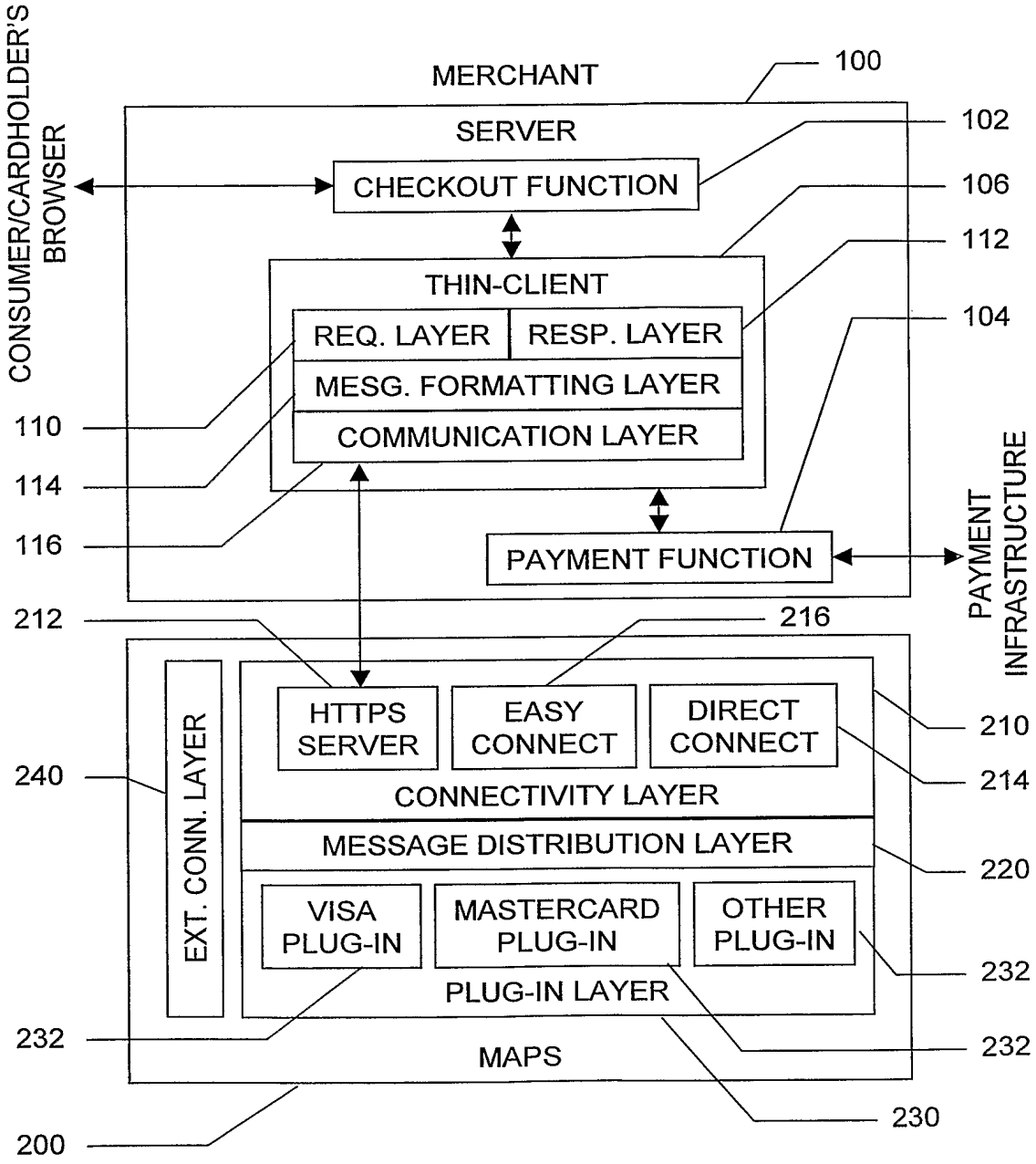

CONSUMER/CARDHOLDER'S BROWSER
MERCHANT
SERVER
100
102
CHECKOUT FUNCTION
106
112
THIN-CLIENT
REQ. LAYER
RESP. LAYER
MESG. FORMATTING LAYER
COMMUNICATION LAYER
104
110
114
116
PAYMENT FUNCTION
PAYMENT INFRASTRUCTURE
212
216
HTTPS SERVER
EASY CONNECT
DIRECT CONNECT
210
214
240
EXT. CONN. LAYER
CONNECTIVITY LAYER
MESSAGE DISTRIBUTION LAYER
220
VISA PLUG-IN
MASTERCARD PLUG-IN
OTHER PLUG-IN
232
PLUG-IN LAYER
232
232
MAPS
230
200

FIGURE 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/18531

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 17/60
US CL :705/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/35-37, 44; 707/100-104

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,070,150 A (REMINGTON ET AL.) 30 MAY 2000, SEE COLUMN 5, LINE 44 TO COLUMN 6, LINE 32.	1-15
A	US 5,884,288 A (CHANG ET AL.) 16 MARCH 1999, SEE COLUMN 2, LINE 33 TO COLUMN 3, LINE 12.	1-15
A	JP 360079466 A (TOSHIBA CORP) 07 MAY 1985, SEE ENTIRE DOCUMENT.	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
19 SEPTEMBER 2003

Date of mailing of the international search report
15 OCT 2003

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
FRANTZY POINVIL
Telephone No. (703) 305-9779

Form PCT/ISA/210 (second sheet) (July 1998)★